AO-106 (Rev. 06/09)-Application for Search Warrant

FILED

NOV 25 2024

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
Information Associated with Snapchat Account "jdubhood" with User ID 9ce01d78-be3e-464e-833e-5ee2128a76af that is Stored at a Premises Controlled by Snap, Inc.

Case No. 24-mj-740-MTS

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 2252(a)(2) and (b)(1)	**Receipt and Distribution of Child Pornography**
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	**Possession of and Access with Intent to View Child Pornography**

The application is based on these facts:

See Affidavit of SA Dustin Carder, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Dustin Carder, HSI
Printed name and title

Subscribed and sworn to by phone.

Date: 11-25-2024

Judge's signature

City and state: Tulsa, Oklahoma

Mark T. Steele, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Information Associated with Snapchat Account "jdubhood" with User ID 9ce01d78-be3e-464e-833e-5ee2128a76af that is Stored at a Premises Controlled by Snap, Inc.	**Case No. _____** **FILED UNDER SEAL**

Affidavit in Support of an Application for a Search Warrant

I, Dustin L. Carder, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with Snapchat account **"jdubhood" with User ID 9ce01d78-be3e-464e-833e-5ee2128a76af** that is stored at a premises owned, maintained, controlled, or operated by Snap, Inc., an electronic communications service and/or remote computing service provider headquartered at 2772 Donald Douglas Loop North in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Snap, Inc. to disclose to the government information (including the content of communications) in its possession, pertaining to the subscriber or customer associated with the Snapchat accounts, as further described in Section I of Attachment B. Upon receipt of the information described

in Section I of Attachment B, government-authorized persons will review the information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since December 2018. I am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's ("FLETC") twelve-week Criminal Investigator Training Program ("CITP") and the sixteen-week Homeland Security Investigations Special Agent Training ("HSISAT") program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex

offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252(a).

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information, including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. Based on my training, research, experience, and the facts as set forth in this affidavit, there is probable cause to believe the identified Snapchat accounts contain evidence, instrumentalities, contraband, and/or fruits of violations of Title 18, United States Code, Sections 2252(a)(2) and (b)(1) (Receipt/Distribution of Child Pornography); and Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) by the account holder.

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States … that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Snap, Inc. from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Characteristics Common to Individuals who Exhibit a Sexual Interest in Children

8. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who sexually exploit children, and who produce, distribute, receive, possess, and/or have access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children

engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity, or from sexualized conversations with children;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media and at times, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images and sexually explicit or suggestive materials in a digital or electronic format in a safe, secure, and private environment, such as a computer or cell phone. These child pornography images are often maintained for several years and are kept close by to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and

then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience, I know such individuals often take their electronic devices and storage media, which contain their collections of child pornography, with them when they move or change residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom. Studies have also shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence

of the crime is often still discoverable for extended periods of time even after the individual "deleted".[1] it;

h. Such individuals also may correspond with and/or meet others to share information and materials. This correspondence from other child pornography distributors/possessors is often concealed, rarely destroyed, and can contain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user's identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may provide a window into the identities of individuals seeking to buy or sell child pornography online by tying the illicit transactions back to the user. Financial information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I

[1] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

know individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers, cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

j. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

Snapchat Background

9. Snapchat is a free mobile application made by Snap, Inc. and is available for download through the Apple App Store and Google Play Store. The Snapchat application is used to share information through photos, videos, and chat messages.

10. To use Snapchat, a user must download the mobile application to their mobile device and sign up using their name and date of birth. The user then selects a username and password. Snapchat then requires an email address or phone number to create an account. A user can also create a vanity name.

11. "Snaps" are photos or videos taken using the camera on an individual's mobile device through the Snapchat application, and may be shared directly with the user's friends, or in a story (explained further below), or chat.

12. A Snapchat user can add Snaps to their "story." A story is a collection of

Snaps displayed in chronological order. Users can manage their privacy settings so that their story can be viewed by all users, their friends, or a custom audience. A user can also submit their Snaps to Snapchat's crowd-sourced service "Our Story," which enables their Snaps to be viewed by all users in Search and Snap Map.

13. "Memories" is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snapchat and may remain in Memories until deleted by the user. Users may encrypt their content in Memories in which case the content is not accessible to Snap, Inc. and cannot be decrypted by Snap, Inc.

14. A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat application using the Chat feature. Snapchat's servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings.

15. If a Snapchat user has device-level location services turned on and has opted into location services on the Snapchat application, Snap, Inc. will collect location data, which will vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the application settings.

16. A Snapchat username is a unique identifier associated with a specific Snapchat account, and it cannot be changed by the user.

17. Basic subscriber information is collected when a user creates a new Snapchat account, alters information at a later date, or otherwise interacts with the Snapchat application. The basic subscriber information entered by a user in creating an account is maintained as long as the user has not edited the information or removed the information from the account.

18. In addition to the information provided by a user to register an account, Snap, Inc. may retain the account creation date and IP address. Further Snap, Inc. also stores a user's Timestamp and IP address of account logins and logouts.

19. For each Snapchat user, Snap, Inc. collects and retains the content and other records described above.

20. Snap, Inc. retains logs for the last 31 days of Snaps sent and received, for 24 hours of posted Stories, and for any unopened Chats or those saved by the sender or recipient. The logs contain meta-data about the Snaps, Stories, and Chats, but not the content. Snap, Inc. may be able to retrieve content of some Snaps.

21. Videos and photos sent and received as Snaps are accessible to users for only a short period of time. If a screenshot is taken of an image by the recipient, the sender is notified. Videos cannot be saved by the recipient. Because of the common belief by Snapchat users that videos and photos cannot be retained by recipients, Snapchat is often used to facilitate and document criminal acts.

22. As explained herein, information stored in connection with a Snapchat account may provide crucial evidence of the "who, what, why, when, where, and

how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

23. The stored communications and files connected to Snapchat account may provide direct evidence of the offenses under investigation.

24. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Snap, Inc. can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and chat logs, documents, and photos and videos (and the data associated with the foregoing, such as location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. This geographic and timeline information may tend to either inculpate or exculpate the account owner by allowing investigators to understand the geographic and chronological context of Snapchat access, use, and events relating to the crime under investigation.

25. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example,

information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

26. Other information connected to the use of Snapchat may lead to the discovery of additional evidence, the identification of co-conspirators, witnesses, and instrumentalities of the crime(s) under investigation.

27. Therefore, Snap, Inc.'s servers are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Snapchat to facilitate and communicate about the crime under investigation.

28. I previously requested that Snap, Inc. preserve any information for the account(s) listed in Attachment A.

Background of NCMEC and the CyberTipline Program

29. The National Center for Missing & Exploited Children ("NCMEC") was incorporated in 1984 by child advocates as a private, non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further the mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program. NCMEC makes

information submitted to the CyberTipline and Child Victim Identification Program available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers ("ESPs"), law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business operations. NCMEC does not act in the capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

30. NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and ESPs can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sex abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. CyberTipline Reports ("CyberTips") are distributed by NCMEC analysts to law enforcement agencies who may have legal jurisdiction in the place that victims and suspects are believed to be located based on information provided in the CyberTips.

Probable Cause

31. On November 6, 2024, I received a request for assistance from Collinsville Police Department ("CPD") Detective/HSI Task Force Officer ("TFO") Josh Ray

regarding NCMEC CyberTip ("CT") 197854489. The Oklahoma State Bureau of Investigation ("OSBI"), who manages and assigns the CTs received throughout the State of Oklahoma, assigned the CT to CPD.

32. CT 197854489 was received by NCMEC on August 18, 2024, at 12:45:24 UTC. The CT was filed by Snapchat regarding username **"jdubhood,"** who had uploaded, saved, or shared a video file of child pornography on their platform on August 17, 2024, at 03:54:24 UTC.

33. Filename **jdubhood-None-ac1a50ac-25b1-59a3-bb1d-4eea13b0f60d~10-15c6714a13-content.mov** with MD5 hash value 0c02af8f76b7c84a9913fc5d94e569a5 was viewed by Snapchat and NCMEC staff. TFO Ray and I have also viewed the file. The video is one-minute, twenty-six seconds (1:26) long and depicts an adolescent or adult male laying on a bed. The male has a partially clothed toddler, who appears to be asleep or drugged, lying face down on the other male's chest. The toddler only has a shirt on, which is pulled up near his shoulders. The older male repeatedly inserts his penis into the toddler's anus, masturbating while it is inserted into the toddler, and when he removes it. This file constitutes child pornography as defined in 18 U.S.C. § 2256.

34. In addition to the username, Snapchat provided additional suspect information for the account: a verified phone number of (918) 694-6779, date of birth of xx/xx/1994, verified email address of "jhood513@me.com," and an IP address of 12.206.137.11. The IP address geo-located to Irving, Texas, which caused the CT to

be originally assigned to the Irving Police Department's ("IPD") Internet Crimes Against Children Task Force.

35. On or about September 11, 2024, IPD Investigator K. Chaisson served a State of Texas administrative subpoena to Apple, Inc. regarding subscriber information related to the "jhood513@me.com" email address, which is serviced by Apple.

36. On or about September 17, 2024, Apple responded to the subpoena and provided the requested information. The customer name is listed as "Joel Hood" with a phone number of (918) 694-6779, and address of 13005 North 135th East Avenue, Collinsville, OK 74021, which is within the Northern District of Oklahoma ("NDOK"). There have been multiple Apple iPhones and iPads associated with the email address.

37. On or about September 11, 2024, Investigator Chaisson served a State of Texas administrative subpoena to AT&T for IP address 12.206.137.11 on 08-17-2024 03:54:24 UTC.

38. On or about September 18, 2024, AT&T responded to the subpoena and provided the requested information. AT&T advised that the IP address is registered to Six Continents Hotels, Inc., with a service address of 11699 East 96th Street North, Owasso, OK 74055, which is also within the NDOK. A Google search revealed that this address belongs to the Candlewood Suites Hotel in Owasso.

39. It appears at this time the CT was sent to OSBI for reassignment, who in turn assigned it to CPD. Utilizing the identifying information provided in the CT as well

as the Apple subpoena return, the suspect was identified as Joel Wyatt HOOD, date of birth xx/xx/1994, with an address of 13005 North 135th East Avenue, Collinsville, OK 74021.

40. On November 7, 2024, TFO Ray drove to the above residence and observed a truck backed in the driveway as well as a 2023 Ford Bronco with Cherokee Nation tag AC3-932. A registration check revealed the vehicle is registered to a George and Reba Wright at the same residence.

41. TFO Ray and I confirmed with the Cherokee Nation tribe that HOOD is a registered citizen of the tribe (Citizen ID: 256196).

42. I queried HOOD in the National Crime Information Center and learned that he is on active probation with the Cherokee Nation. The return provided contact information for HOOD's probation officer. On November 7, 2024, I contacted HOOD's probation officer and learned that HOOD was on probation for a Driving Under the Influence charge. The probation officer confirmed that HOOD lives at 13005 North 135th East Avenue in Collinsville but provided a different phone number for him. I also learned that HOOD resides at the location with his grandparents, George and Reba Wright.

43. On November 7, 2024, I electronically served an administrative Department of Homeland Security ("DHS") summons to U.S. Cellular for subscriber information related to phone number (918) 694-6779. This is the phone number associated with the "jdubhood" Snapchat account listed on the CT.

44. On November 8, 2024, U.S. Cellular responded to the summons and provided the requested information. U.S. Cellular records indicate that the phone number was active from January 8, 2021, until March 8, 2024, at which time it was suspended. I confirmed with U.S. Cellular that the number is still currently suspended. The account owner is Roxanna Krebs, date of birth xx/xx1958; her listed address is 6780 South 97th West Avenue, Sapulpa, Oklahoma 74066. This address is also located within the NDOK. The connection between Krebs and HOOD, if any, is unknown at this time.

45. On November 11, 2024, I electronically served an administrative DHS summons to Snap, Inc. for subscriber information related to Snapchat username jdubhood.

46. On November 14, 2024, Snap, Inc. responded to the summons and provided the requested information. **Username jdubhood is associated with User ID 9ce01d78-be3e-464e-833e-5ee2128a76af**. The account is associated with verified email address "jhood513@me.com," and verified phone number (918) 694-6779. The account was created on March 4, 2013, and is still active. The account was last active on August 16, 2024. The account was "locked" on August 17, 2024, four minutes after HOOD had uploaded, saved, or shared the video file of child pornography on Snapchat.

47. I also observed in the returned subscriber data that HOOD set his "home" location as GPS coordinates 36.343025, -95.823036. Upon entering these coordinates

into Google, I noted that those are the coordinates for HOOD's address of 13005 North 135th East Avenue, Collinsville, OK 74021.

48. I am requesting account data and contents for August 1, 2024, through August 17, 2024, the date the account was locked.

Information to be Searched and Things to be Seized

49. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Snap, Inc. Because the warrant will be served on Snap, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

50. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Snap, Inc. to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

51. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information

within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

52. Based on the information above, I submit that there is probable cause to believe that there is evidence of violations of Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) associated with the Snapchat account described in Attachment A.

53. I request to be allowed to share this affidavit, and the information obtained from this search (to include copies of digital media) with any government agency, to

include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

Dustin L. Carder
Special Agent
Homeland Security Investigations

Sworn and subscribed by telephone this 25 day of November 2024.

MARK T. STEELE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the Snapchat account **Username jdubhood is associated with User ID 9ce01d78-be3e-464e-833e-5ee2128a76af** which is stored at the premises owned, maintained, controlled, and/or operated by Snap, Inc., a company headquartered in Santa Monica, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Snap, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap, Inc., regardless of whether such information is located within or outside the United States, and including any messages, records, files, logs, photographs, videos or other information that has been deleted but is still available to Snap, Inc., or has been confirmed preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snap, Inc. is required to disclose the following information to the government for each account listed in Attachment A:

A. All stored communications and other files in Snap, Inc.'s possession (including account access information, event histories including dates and times, connection dates, times and locations, connection IP information, message content, graphics files, attachments, etc., further detailed below), whether physical, stored on electronic media, or temporarily extant on any computer or server, reflecting communications to or from the Snapchat account identified in Attachment A;

B. All subscriber information, including Snapchat username vanity names, email addresses, phone numbers, full name, physical address, and other personal identifiers;

C. All information pertaining to the creation of the account, including date and time of creation, IP address used to create the account, and all subscriber

information provided at the time the account was created;

D. Timestamp and IP address of all account logins and logouts.

E. Logs of all messages and all files that have been created and Snaps sent or accessed via the Snapchat account identified in Attachment A, or that are controlled by user accounts associated with the Snapchat account;

F. The account name, vanity name, identifiers and all available subscriber information for any other Snapchat account(s) associated with the Snapchat account listed in Attachment A;

G. All content, records, connection logs, and other information relating to communications sent from or received by the Snapchat account identified in Attachment A from August 1, 2024, through August 17, 2024, including but not limited to:

1. Transmitter/Sender identifiers (i.e., addresses and/or IP address);
2. Connection date and time;
3. Method of Connection (telnet, ftp, http);
4. Data transfer volume;
5. Username associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
6. Account subscriber identification records;
7. Other user accounts associated with, referenced in, or accessed by the

Snapchat account identified in Attachment A;

8. Address books, contact lists and "my friends";

9. Records of files or system attributes accessed, modified, or added by the user;

10. All records and other evidence relating to the subscriber(s), customer(s), account holders(s), or other entity(ies) associated with the Snapchat account identified in Attachment A, including, without limitation, subscriber names, user names, screen names or other identities, addresses, residential addresses, business addresses, and other contact information, telephone numbers or other subscriber number or identifier number, billing records, information about the message and Snaps and all information length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content associated with or relating to postings, communications and any other activities to or through the Snapchat account listed in Attachment A, whether or such records or other evidence are in electronic or other form;

11. All records pertaining to communications between Snap, Inc. and the

user(s) of the Snapchat account identified in Attachment A regarding the user or the user's Snapchat account, including contacts with support services and records of actions taken;

12. The content of all messages and Snaps sent, received, saved, stored, or otherwise preserved.

13. Accounts linked by: cookie; recovery, alternate, forwarding, or login e-mail address or phone number; phone number; creation IP address; and access or login IP address.

Snap, Inc. is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, instrumentalities, contraband, and/or fruits of violations of Title 18 U.S.C. §§ 2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), collectively referred to as the "**Target Offenses,**" from August 1, 2024, through August 17, 2024, including for each account or identifier listed on Attachment A:

a. Messages, communications, records, and files associated with or attached to email or chat messages, and transactional data that constitute evidence of, or that may have been used to facilitate, or that were capable of being used to commit or further the **Target Offenses**;

b. Images, videos, and other files depicting children engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c. Communications that pertain to or that are evidence of the production, advertisement, distribution, receipt, or possession of child pornography, or accessing with the intent to view child pornography;

d. Communications between the Snapchat accounts identified in Attachment A and others, which constitute evidence of, or that may have been used to facilitate, or that were capable of being used to commit or further the **Target Offenses**, from August 1, 2024, through August 17, 2024;

e. Evidence indicating the times, geographic locations, and electronic devices from which the Snapchat account listed in Attachment A was accessed and used, to determine the chronological and geographical context of the Snapchat account access, use, and events relating to the crime(s) under investigation and to the Snapchat account user;

f. Evidence indicating the Snapchat account owner's state of mind as it relates to the crime(s) under investigation;

g. The identity of the person(s) who created or used the Snapchat account identified in Attachment A, including records that help reveal the whereabouts of such person(s);

As used above, the terms "documents," and "communications," refers to all content regardless of whether it is in the form of pictures, videos, audio records, text communications, or other medium and whether in draft or completed form and whether sent or received;

As used above, the terms "records" and "information" includes all forms of data stored by Snap, Inc., including IP addresses, toll records, and account identifying information.